BY ORDER OF THE COMMANDER,
PACIFIC AIR FORCES

AIR FORCE INSTRUCTION 31-501

PACIFIC AIR FORCES COMMAND
Supplement 1

11 JUNE 2004

Security

PERSONNEL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ PACAF/SFOI
(Mr. Charles E. Curnutte)
Supersedes AFI 31-501_PACAFSUP1,
9 September 1994

Certified by: HQ PACAF/SFO
(Maj Joshua D. Fowler)
Pages: 15
Distribution: F

AFI 31-501, 1 August 2000, is supplemented as follows: This supplement applies only to Air National Guard (ANG) United States Title 10 status. It does not apply to the Air Force Reserve. This instruction may be supplemented at wing level.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1.1.2. Submit requests for waivers, inquiries, and recommendations for changes through the servicing ISPM to PACAF/SFO, 25 E. St., Bldg 1102, Suite M310, Hickam AFB, HI 96853-5439.

2.5. Effective 1 October 2003, OPM will conduct all DoD military and civilian Personnel Security Investigations (PSIs).

2.9. (Added) . At PACAF installations, the Security Forces unit is the Servicing Security Activity.

3.2.1. For newly-hired civilian employees assigned to non-critical sensitive positions, the Civilian Personnel Flight (CPF) will submit a request for an Access National Agency Check with Written Inquiries and Credit Check (ANACI) and Single Scope Background Investigation (SSBI) for Top Secret positions.

3.5. Periodic Reinvestigations (PR) are required for civilian employees in positions coded as 5/SSBI and 7/ANACI positions.

3.11. Review JCAVs to verify status of investigations.

3.11.2.3. When initiating request, verify confirmed receipts for ANACIs through the supporting CPF and JPAS.

3.12. The authority to approve requests for Limited Access Authorization's (LAAs) is delegated to the Chief, Policy Branch, PACAF/SFOP. Authorized requesters will contact PACAF/SFOP to obtain SSNs for foreign nationals. This will assist in tracing investigation status. A record of the SSN will be maintained with the case file to ensure it is used only one time.

3.12.1.1. (Added) . LAAs must be limited to people having a special skill or technical expertise essential to fulfilling a DoD requirement that cannot be filled by a U.S. citizen.

3.12.1.2. (Added) . LAAs must not be granted to people who perform routine administrative or other support duties, such as secretaries, clerks, or drivers, unless it has been clearly established that a U.S. citizen cannot perform the duties.

3.12.1.3. (Added) . LAA recipients will not be granted uncontrolled access to areas where classified information is stored or discussed.

3.12.1.4. (Added) . Classified information must be maintained in locations under continuous control and supervision of a cleared U.S. person. Note: Do not give LAA recipients security container combinations.

3.12.1.5. (Added) . The scope of access must be specifically described in the LAA nomination request. Access to classified information not specifically addressed in the nomination request constitutes a compromise of classified information.

3.12.1.6. (Added) . LAA recipients cannot be designated as a courier or escort classified information outside the location in which access is permitted unless accompanied by a cleared U.S. person.

3.12.1.7. (Added) . Commanders must plan LAA requirements accordingly. The average time from the decision to initiate an LAA request through final adjudication is 9 to 15 months.

3.12.2. LAA Access Levels.

3.12.2.1. (Added) . LAAs are only authorized at the SECRET or CONFIDENTIAL level.

3.12.2.2. (Added) . Commanders may never grant interim access for LAAs.

3.12.2.3. (Added) . The information released to the LAA recipient must be releasable to the person's country or countries of citizenship.

3.12.2.4. (Added) . Access must be limited or related to a specific program or project. The LAA must be terminated or re-justified upon completion of the project or program.

3.12.3. (Added) . LAA Requirements.

3.12.3.1. (Added) . The installation ISPM, the Chief of Security Forces (CSF), approves unit LAA requests. After approval, send request to PACAF/SFO. (See **Attachment 24 (Added)** Sample Memorandum for Initial LAA Pre-Approval.)

3.12.3.2. (Added) . PACAF/SFO pre-approves all LAA requests. Note: SF pre-approval does not authorize or constitute access to classified information; it is intended to give units permission to initiate a single-scope background investigation (SSBI) request.

3.12.3.3. (Added) . A favorably completed and adjudicated SSBI is required before access can be granted.

3.12.3.4. (Added) . A PR must be conducted every five years based on the AF Form 2584 Investigation Date in Block 9.

3.12.3.5. (Added) . LAAs must be re-certified annually by PACAF/SFO. Recertification requests are due to PACAF/SFO by 1 Oct each year. PACAF/SFO will not recertify LAAs if the required PR has not been submitted in accordance with paragraph **3.12.3.4. (Added)** Non-recertification will result in LAA suspension. (See **Attachment 25 (Added)**, Sample Recertification Request Letter.)

3.12.3.6. (Added) . All requests for LAAs must contain a detailed justification and plan describing the following:

3.12.3.6.1. (Added) . Location of classified information (security container, vault, etc.) in relationship to the location of the foreign national.

3.12.3.6.2. (Added) . Nature of access must be clearly defined. Statements such as "the person is needed to translate host nation communications and correspondence or needed to execute mission requirements" are too broad and generic and will result in disapproval of LAA requests.

3.12.3.6.3. (Added) . Compelling reasons for not employing a cleared or eligible U.S. citizen.

3.12.3.6.4. (Added) . Provide a synopsis of an annual continuing evaluation program to evaluate the person's continued trustworthiness and eligibility for access.

3.12.3.6.5. (Added) . A plan to control access to secure areas, and to classified and controlled unclassified information.

3.12.3.7. (Added) . LAA recipients must sign an SF 312, *Nondisclosure Agreement*, before being granted access to classified information.

3.12.3.8. (Added) . Unless prohibited by host nation laws, LAA recipients must agree, in writing, to undergo a polygraph if requested by competent authority before being granted access to classified information. Non-US citizens who decline a request for a polygraph shall be ineligible for LAAs or, if an LAA has already been approved, access to classified information shall immediately be terminated. If a request for a polygraph examination is not appropriate, non-US citizens shall not be asked to undergo a polygraph and their eligibility to maintain LAAs will be based on investigation and review of available personal data.

3.12.3.9. (Added) . LAA recipients must sign an AF Form 2587, *Security Termination Statement,* when they no longer require access to classified information or terminate their service. (See **Attachment 26 (Added)**, Sample Memorandum for LAA Termination.)

3.12.3.10. (Added) . Unit commanders must immediately notify the ISPM when an LAA is terminated or suspended. The ISPM will then notify PACAF/SFO.

3.12.3.11. (Added) . Changes to LAA (nature of access or level of access) information must be forwarded to PACAF/SFO for approval. Recommend units attach a separate memo to the initial LAA.

3.12.3.12. (Added) . PACAF/SFO must submit an annual LAA report to AFCAF/INS NLT 1 November each year.

3.12.4. (Added) . LAA Case File/Records Maintenance.

3.12.4.1. (Added) . LAA files/records must be maintained for five years from the date of LAA termination.

3.12.4.2. (Added) . As a minimum, the LAA file/record must contain the following:

3.12.4.2.1. (Added) . The identity of the LAA recipient, to include: full name, date and place of birth, current citizenship, SSAN (if applicable), and national identification number.

3.12.4.2.2. (Added) . The person's status as an immigrant alien or foreign national. Note: If the person is an immigrant alien, annotate the date and place status was granted.

3.12.4.2.3. (Added) . The LAA classification level, e.g., SECRET or CONFIDENTIAL.

3.12.4.2.4. (Added) . Date and type of most recent background investigation/PR and the investigating agency.

3.12.4.2.5. (Added) . Whether a polygraph examination was conducted; if so, the date and administering agency.

3.12.4.2.6. (Added) . The nature and identity of the classified program materials to which access is authorized and the precise duties performed.

3.12.4.2.7. (Added) . The compelling reason for granting access to classified information.

3.12.4.2.8. (Added) . A copy of the most recent Personnel Security Investigation, or computer disk containing the information.

3.12.4.2.9. (Added) . The SF 312, *Nondisclosure Agreement.*

3.12.4.2.10. (Added) . A copy of the most recent AF Form 2583, *Request for Personnel Security Action*.

3.12.4.2.11. (Added) . A copy of the most recent AF Form 2584, *Record of Personnel Security Investigation and Clearance.*

3.12.4.2.12. (Added) . The most recent annual PACAF/SFO Recertification memo.

3.12.4.2.13. (Added) . Written acknowledgment to take a polygraph test when directed by competent authority, e.g. unit commander, AFOSI, DSS.

3.12.4.2.14. (Added) . An AF Form 2587, *Security Termination Statement,* when access to classified information is no longer required, e.g., retirement, program completion.

3.12.4.2.15. (Added) . Any other unit or official correspondence pertaining to LAA status, e.g. re-justification of access, suspensions.

3.12.5. (Added) . The LAA Process.

3.12.5.1. (Added) . After determining mission requirements cannot be successfully accomplished without employing a foreign national, the unit commander submits an initial LAA pre-approval request to the installation ISPM for review and concurrence.

3.12.5.2. (Added) . If the installation ISPM concurs with the request, he/she endorses it and forwards it to PACAF/SFO for pre-approval. The ISPM must ensure unit commanders accurately depict their LAA requirements and provide detailed justification, especially in the area of the nature of access (specific nature of work regarding classified information).

3.12.5.3. (Added) . If PACAF/SFO pre-approves the LAA request, the memorandum is endorsed and sent to AFCAF/INS, with a courtesy copy to the requesting ISPM.

3.12.5.4. (Added) . After PACAF/SFO pre-approves the LAA request and forwards the "Dummy" SSAN, the requesting unit can initiate personnel security clearance requirements, e.g., EPSQ or SF 86, AF Form

2583. Follow locally-established procedures for distributing paperwork to the Security Forces and AFOSI detachment.

3.12.5.5. (Added) . AFOSI will conduct their portion of the LAA recipient's SSBI and forward the results to the Office of Personnel Management (OPM). OPM will forward the case file to AFCAF/INS for adjudication.

3.12.5.6. (Added) . If the AFCAF/INS favorably adjudicates the LAA, they will forward an AF Form 2584 to PACAF/SFO. PACAF/SFO will endorse the adjudication and forward it to the installation ISPM, who, in turn, forwards it to the requesting unit.

3.12.5.7. (Added) . Upon completion of all the above actions (Paras **3.12.5.1. (Added)** to **3.12.5.6. (Added)**), the unit commander can grant access to classified information as soon as the LAA recipient signs the SF 312, *Nondisclosure Agreement,* and consents (in writing) to take a polygraph when directed by competent authority.

3.12.5.8. (Added) . Self-Inspections will be conducted annually using **Attachment 27 (Added)**, LAA Self-Assessment Checklist, NLT 30 Nov of each year.

3.14.2. Personnel Security Investigations (PSIs) for consultants will be submitted by the Security Forces authorized requester. Consultants are not categorized as Contractors.

3.15. The approving authority's authorization will be maintained by the servicing unit security manager.

3.24.1. DoD civilians require a National Agency Check with Written Inquiries (NACI) for unescorted entry to restricted areas.

3.24.4. The definition of OPM civilians and federal employees is "DoD civilians." NACs are required for Non-DoD civilians. For this purpose, a federal employee is defined as a non-appropriated fund (NAF) employee.

3.24.10.1. (Added) . The security manager must ensure contractors have the proper personnel security investigation (PSI) before signing the AF Form 2586, *Unescorted Entry Authorization Certificate*. If there is no record in JPAS, contact the ISPM for assistance in checking Defense Industrial Security Clearance Office (DISCO) records. Submit PSI to the appropriate investigative agency if there is no record of investigation.

3.27.3.7.3. (Added) . Unit commanders are responsible for favorable suitability determinations. The commander will use the adjudication guidelines in DoD 5200.2-R, Section 2-200.

3.28. Personnel in positions requiring personnel security investigations will submit the appropriate update before the expiration date of the investigation. Top Secret positions must be current within 5 years and Secret positions must be current within 10 years. Failure to complete the appropriate reinvestigation shall result in termination of the individual's security clearance and/or assignment to sensitive duties.

5.2.1. The following organizations at each PACAF installation are designated authorized requesters:

5.2.1.1. (Added) . Security Forces are authorized requesters for positions requiring access to classified information, unescorted entry to restricted areas, PRP, NIPRNET (LAN) access, and presidential support.

5.2.1.2. (Added) . Human Resource Offices (HROs) are authorized requesters for positions of trust and child-care NAF employees.

5.2.1.3. (Added) . CPFs are authorized requesters for NACIs for non-sensitive positions and for ANACIs when civilian employees are initially hired to non-critical sensitive positions.

5.5. ISPMs submit, through PACAF/SFO, requests with justification for priority handling to HQ USAF/XOFI for approval.

7.1.2.1. IAW SAF/AA Memo, 11 October 2002, Personnel Security Investigations Requirements, position coding will be assigned by the type of investigation required for mission purposes versus security clearance requirements. The term security access requirement (SAR) has been replaced with position coding. Upgrade of a position from Secret to Top Secret or identification of a new Top Secret requirement requires 3-Star/civilian equivalent approval. (See **Attachment 28 (Added)**, Conversion Table, Security Access Requirement (SAR) Top Position Coding.)

7.1.2.1.1. (Added) . PACAF/CV may delegate authority to wing commanders to approve new Single Scope Background Investigation (SSBI) requirements. This will be determined on a case-by-case basis. The wing commander may submit their request to PACAF/CV and courtesy copy PACAF/SFOP.

7.1.2.2. Records of the annual review of Position Codes will be subject to review during annual program reviews by the ISPM.

7.3.1. PCS or TDY orders should indicate clearances as Top Secret or Secret do not use DCID 6/4. Access to SCI must be verified through Special Security Office (SSO).

7.4.2.5.1. (Added) . PACAF/SF is the JPAS account manager for the MAJCOM. An individual must have a National Agency Check, Local Agency Checks and Credit (NACLC) or Access National Agency Check and Inquiries (ANACI) investigation completed before a JPAS account is established.

7.4.2.6.5. Level 5 “User” designation may be given to security managers who serve more than one PAS Code.

7.4.2.8. Local installation account managers will only be assigned to personnel within the security forces unit who manage the Personnel Security Program. Normally there will be only one primary and one alternate account manager for the installation. Local account managers will establish user accounts. Systems administrators do not establish user accounts.

7.4.2.8.1. (Added) . Servicing ISPM will manage their local JPAS account (Level 5, 6, and 7).

7.4.2.8.2. (Added) . Servicing ISPM will review JPAS accounts quarterly for accuracy.

7.5.1. (Added) . IAW HQ USAF/XOF memo 25 November 2002, positions identified for deployment will be assigned a NACLC, requiring access to Secret information for the in-country threat briefing. SSBIs will not be authorized for purposes of Top Secret “just in case of” deployment.

8.1.1. Consult the base Information Security Program Manager (ISPM) as needed for technical assistance in this area. The ISPM will coordinate with the installation Staff Judge Advocate, Director of Personnel and AFOSI for monthly updates and information pertaining to SIFs. Information pertaining to an individual under investigation by AFOSI will be coordinated discreetly with the ISPM unless the notification will jeopardize the investigation. Information release is at the discretion of AFOSI.

8.2.1.3. Determination for establishment of a SIF is on a case by case basis, normally within 20 calendar days of receipt of unfavorable information (as soon as possible if SCI access is involved). However, if the commander has sufficient reason to doubt the validity of unfavorable information, the decision to establish a SIF and notification to the CAF may be extended up to 45 calendar days.

8.2.2.5.1. Employment suitability determinations are required as part of SIFs for civilian employees. Commanders or staff agency chiefs are responsible for these determinations with the assistance of the Civilian Personnel Flight (CPF).

8.6.2. Submit appeals through the servicing ISPM.

8.6.4. Submit rebuttals through the servicing ISPM.

11.1.4. The Director of Security Forces, PACAF/SF, develops personnel security policy for PACAF. PACAF/SFOP will coordinate management of HQ PACAF Personnel Security program with the 15th Security Forces Squadron.

11.1.4.1. (Added) . Identify servicing ISPM oversight procedures in local supplement.

12.1.1. Request for DCII access will be routed through PACAF/SFO to the CAF.

Attachment 24 (Added)

SAMPLE MEMORANDUM FOR INITIAL LAA PRE-APPROVAL

MEMORANDUM FOR (INSTALLATION CSF and ISPM) or (PACAF/SF)

FROM: (Unit Commander)

SUBJECT: Initial Limited Access Authorization (LAA) Pre-Approval Request

1. Request initial LAA pre-approval for (name). The LAA is required in support of DoD mission requirements. We provide the following information:

a. Full Name:

b. Date and Place of Birth:

c. Current Citizenship: (if the person maintains dual-citizenship, list both)

d. Status of Individual (immigrant alien, foreign national, etc.): Note: If an immigrant alien, provide date and place where status was granted.

e. Personal Identification #: (SSAN or foreign country identification number)

f. LAA Access Level: (SECRET or CONFIDENTIAL)

g. Nature of Access (list specific duties and program responsibilities):

h. Compelling Reason for Granting Access:

i. Describe the Location of Classified Material in Relationship to the Location of the Foreign National:

j. The Compelling Reason for Not Employing a Cleared U.S. Citizen in the Position:

k. Synopsis of the Unit's Annual Continuing Assessment Program to Evaluate the Individual's Trust-worthiness and Eligibility for Access:

l. Unit's Plan to Control Access to Secure Areas and Classified and Controlled Unclassified Information.

m. Will the Person Consent (in Writing) to a Counterintelligence-Scope Polygraph if Directed by Competent Authority? (Yes or No) LAA Recipient's Initials: _____

n. Does the Recipient Agree to Sign an SF 312, *Nondisclosure Agreement*? (Yes or No)

LAA Recipient's Initials: _____

2. I understand LAA can not be granted until the recipient's investigation is completed and favorably adjudicated by AFCAF/INS, and the recipient signs a SF 312, *Nondisclosure Agreement,* and agrees in writing to undergo a polygraph examination if directed by competent authority. LAA will be immediately terminated when no longer operationally required or suspended if circum-stances warrant such a decision. My POC is _____, DSN _____.

Unit Commander's Signature Element

1st Ind (if applicable), ISPM's Address Element

MEMORANDUM FOR PACAF/SF

I concur/do not concur with initial LAA request.

ISPM'S Signature Element

Attachment 25 (Added)

SAMPLE RECERTIFICATION REQUEST LETTER

MEMORANDUM FOR (INSTALLATION CSF and ISPM) or (PACAF/SF).

FROM: (Unit Commander)

SUBJECT: Annual Limited Access Authorization (LAA) Recertification Request

1. Request annual LAA recertification for (name). We provide the following information:

a. Full Name:

b. Date and Place of Birth:

c. Current Citizenship: (if recipient maintains dual-citizenship, list both)

d. Status of Individual (immigrant alien, foreign national, etc): Note: If an immigrant alien, provide date/place where status was granted.

e. Personal Identification #: (SSAN or foreign country identification number)

f. Date and Type of Investigation (include investigative agency):

g. LAA Access Level: (SECRET or CONFIDENTIAL)

h. Are Access Requirements and Duties the Same as the Initial LAA Pre-Approval Request? (Yes or No) If no, specifically describe and re-justify access requirements.

i. Does the LAA Recipient Consents (In Writing) to Take a Counterintelligence-Scope Polygraph, if Directed by Competent Authority: (Yes or No) If applicable, date of last polygraph examination:_____

j. Individual Has Signed a Nondisclosure Statement? (Yes or No), Date:_____

k. Has a Periodic Reinvestigation (PR) Been Accomplished Within Five Years? (Yes or No) Date of last PR: _____

2. The LAA is required in support of DoD mission requirements. LAA will be immediately terminated when no longer operationally required or suspended, if circum-stances warrant such a decision. My POC is _____, DSN _____.

Unit Commander's Signature Element

1st Ind (if applicable), ISPM's Address Element

MEMORANDUM FOR PACAF/SF

I concur/do not concur with the LAA recertification request.

Attachment 26 (Added)

SAMPLE MEMORANDUM FOR LAA TERMINATION

MEMORANDUM FOR (Installation CSF and ISPM) or (PACAF/SF)

FROM: (Unit Commander)

SUBJECT: Limited Access Authorization (LAA) Termination

1. Request LAA termination for (name). We provide the following information:

a. Full Name:

b. Date and Place of Birth:

c. Current Citizenship: (if the person maintains dual-citizenship, list both)

d. Status of Individual (immigrant alien, foreign national, etc.): Note: If an immigrant alien, provide date/place where status was granted.

e. Personal Identification #:

f. LAA Classification Level:

g. Nature of Access (list specific duties and program responsibilities):

h. Reason for LAA Termination:

i. Individual Has Signed a Security Termination Statement? (Yes or No), Date:_____

2. As required by DoD 5200.2-R, the LAA file/record will be maintained for five years from the date of LAA termination. My POC is _____, DSN _____.

Unit Commander's Signature Element

1st Ind (if applicable), ISPM's Address Element

MEMORANDUM FOR PACAF/SF

I concur/do not concur with the LAA termination request.

ISPM's Signature Element.

Attachment 27 (Added)

LAA SELF-ASSESSMENT CHECKLIST

LAA SELF-ASSESSMENT CHECKLIST	
A4.1. Are commanders, supervisors, security managers, and co-workers aware of LAA requirements, restrictions, and associated limitations?	DoD 5200.2-R, Para 3-402a
A4.2. Has the unit commander established controls to ensure the LAA program is effectively managed and controlled?	DoD 5200.2-R, Para 3-402 b, c, and d
A4.3. Are LAA recipients granted interim access, pending final adjudication? – ***NOT AUTHORIZED***.	DoD 5200.2-R, Para 3-402c(1)
A4.4. Has the unit commander established a continuous evaluation process to ensure LAAs are effectively managed and controlled?	DoD 5200.2-R, Para 3-402d(7)(c)
A4.5. Are LAA periodic reinvestigations (PR) accomplished every ***five*** years?	DoD 5200.2-R, Para 3-402d(6)
A4.6. Are LAA annual recertifications submitted to PACAF/SFO by 1 Oct of each year?	PACAF Sup 1, Para **3.12.3.12. (Added)**
A4.7. Is LAA correspondence prepared in accordance with **Attachment 1** through **Attachment 3**?	PACAF Sup 1, Para **3.12.5. (Added)**
A4.8. Are LAA files/records maintained for ***five*** years after the LAA is terminated?	DoD 5200.2-R, Para 3-402f(1)
A4.9. Did the LAA recipient sign the SF 312 before he/she was granted access to classified information?	PACAF Sup 1, Para **3.12.3.7. (Added)**
A4.10. Do LAA recipients consent, in writing, to undergo a polygraph test before they are granted access to classified information?	DoD 5200.2-R, Para 3-402, f(4)
A4.11. Did the LAA recipient sign an AF Form 2587 after the LAA was terminated?	PACAF Sup 1, Para **3.12.4.2. (Added)**
A4.12. Are LAAs terminated or re-justified upon program/project completion?	PACAF Sup 1, Para **3.12.3.10. (Added)**
A4.13. Are LAA changes and/or re-justifications sent to PACAF/SFO for review and approval before the LAA recipient is granted access to classified information?	PACAF Sup 1, Para **3.12.3.11. (Added)**
A4.14. Is LAA strictly limited to the specific scope of access requested in the initial LAA memorandum?	PACAF Sup 1, Para **3.12.1.5. (Added)**

Attachment 28 (Added)

CONVERSION TABLE
SECURITY ACCESS REQUIREMENT (SAR) TOP POSITION CODING

SAR	POSITION CODING
0 or Blank (no access)	8 NACI (civilian) 9 NAC
1 Secret	6 NACLC (military) 7 ANACI (civilian)
2 Top Secret	5 SSBI
3 SIOP-ESI	5 SSBI
3 AFOSI	5 SSBI
3 DoD Courier	5 SSBI
3 Presidential Support	5 SSBI Category 1 & 2 6 NACLC (military) Category 3 7 ANACI (civilian) Category 3
S SCI	5 SSBI
4 Child Care	9 NAC

NOTE: This table updates AFI31-501, Table A3.7. The above table is a guide to convert positions from the Security Access Requirement system to the new Position Coding system. Some conversations will not be one for one and may vary depending on the situation. For example, Presidential Support Category 1 and 2 requires an SSBI, and Category 3 requires a NACLC. SAR codes “0” or “Blank” could possibility be coded other than 8 or 9, depending on the original reason coded 0 or blank (possible miscoding). When converting positions, it is possible a position will convert to another position code because under the new system, every position is coded with an investigation requirement.

ALBERT F. RIGGLE, Colonel, USAF
Director of Security Forces